TESTIMONY OF

GREGORY SCHAFFER
CHIEF SECURITY OFFICER
ALLTEL COMMUNICATIONS, INC.

BEFORE THE
COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON OVERSIGHT & INVESTIGATIONS
U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 29, 2006

Introduction

Chairman Whitfield, Ranking Member Stupak, and Members of the Subcommittee, thank you for the opportunity to address the Subcommittee on the critically important topic of protecting customer information. I commend you for the leadership you have shown in attempting to address a problem that jeopardizes the privacy of your constituents and our customers.

My name is Gregory Schaffer. I am the Chief Security Officer at Alltel Communications, Inc. ("Alltel"), a position I have held since March 2006. Before that I served as Alltel's Chief Information Security Officer. I came to Alltel in 2004 with substantial relevant experience in information security issues. Not only did I serve as a Director in the Cybercrime Prevention and Response Practice at PricewaterhouseCoopers for four years prior to joining Alltel, I also prosecuted computer hacking, illegal wiretaps and economic espionage crimes while working in the Department of Justice's Computer Crime and Intellectual Property Section. My hiring, and the company's commitment to the development of an enterprise wide security office responsible for both physical and information security, demonstrates Alltel's serious commitment to protecting its customer data.

Before I discuss the ways in which Alltel implements measures to protect our customers' records from pretexters, data brokers, and other threats, let me briefly tell you about Alltel.

About Alltel

Alltel is headquartered in Little Rock, Arkansas, and owns and operates a wireless network that covers over half of the continental United States. We do not provide any services outside the United States. Alltel offers a variety of wireless products to businesses and consumers, including: postpaid wireless calling plans, prepaid wireless service, wireless GPS vehicle tracking for business customers, and various data applications. Despite the size and complexity of our physical network, our customer base of over eleven million is far smaller and much more diffuse than the national carriers, such as Sprint, Verizon, and Cingular, whose customers and networks are concentrated in urban centers. Indeed our customers, and the over 19,000 employees in thirty-five states that support them, are primarily located in rural America. This explains, in part, why we are also a major roaming partner to much of the wireless industry, providing roaming capabilities in rural areas for both GSM and CDMA network providers. If you spend any significant time using your cell phone beyond the reach of a major interstate highway in certain parts of the United States, you probably have made use of Alltel's network.

So, notwithstanding our smaller customer base, Alltel is faced with all of the same complex challenges involved in implementing effective security controls that confront the larger national carriers. As I will explain, we have addressed those challenges aggressively by devoting significant resources to implementing standardized data security policies, procedures and technologies across our entire enterprise.

Recognition of the Data Broker/Pretexting Problem

Alltel takes the threats presented by data brokers and others who use pretexting methods to attempt to obtain customer data without authorization very seriously. Though actions by the Federal Communications Commission, Federal Trade Commission, certain state legislatures and Attorneys General, and private litigation have caused some data brokers to cease operations, many data brokers still remain in business and continue to develop new and inventive ways to attempt to gain access to customer records. But data brokers are not the only ones trying to use pretexting methods to obtain customer records. Non-commercial pretexting attempts by other unauthorized persons, such as ex-spouses, hackers, or "so-called" friends are also a problem.

Understanding the current methods employed by all of these types of actors to obtain unauthorized access to records is instructive, but at Alltel we also worry about anticipating future techniques. We know that any static approach to preventing unauthorized access -- whether self-directed or imposed by regulation -- will quickly become obsolete. Instead, our practices must have the flexibility to evolve to meet constantly changing technical and social engineering threats. Part of my job is devoted to strategically anticipating those future threats and designing methods and practices to defeat them.

Other Challenges Related to Data Protection

Please keep in mind, however, that effectively serving customers requires Alltel to carefully balance the need to protect customer data with the customers' demand for efficient and expeditious customer service. Imposing overly complicated security measures can significantly extend customer service response times and can frustrate legitimate customer account inquiries. Alltel is constantly evaluating its data security and customer validation methods to balance the need for data protection with our commitment to providing our customers with timely access to their account information when they are at home or on the road, and whether they access Alltel by phone, by computer, or by visiting one of our physical locations. Generally, the stricter our verification methods become, the more likely it is that legitimate customers will be denied access to their information in a timely manner, resulting in customer dissatisfaction and increased expenses to Alltel and our customers.

How Alltel Protects Customer Information

In order to achieve a reasonable balance of accessibility and security, Alltel has invested significant resources in our security and privacy programs. As subcommittee staff knows, Alltel has demonstrated its commitment to protecting customer data by adopting an *Enterprise*

Information Security Policy Framework that formally established both the responsibilities of the Chief Security Officer Position and the Enterprise Security Office, which currently comprises over 100 Alltel employees and is Alltel's "one-stop shop" for security and privacy issues. Alltel has also invested in new technologies to prevent unauthorized access to customer data and refined its customer, employee, and agent authentication policies.

The Enterprise Security Office is responsible for defining and executing Alltel's Enterprise Information Security Program, the goal of which is to adequately protect all of the data collected, generated, stored, managed, and otherwise handled by Alltel. Under that Program, the Chief Security Officer has been given express responsibility for Information Security Strategy, Policy Management, Coordination and Enforcement, Security Awareness and Training, Security Research, Security Recommendations, Security Scanning, Security Monitoring and Log Review, Incident Response, Investigation and Notifications, Security Testing, Coordination of Security Resources, and chairing the company's Security Steering Committee comprising senior level executives. By creating a senior executive position to focus exclusively on security-related issues, Alltel has modified its corporate structure to ensure that these issues will be given the highest level of attention and resources.

Technology Investments

Alltel has made significant investments in various technologies to ensure that its information security infrastructure adequately protects customer data, not just from pretexters, but also from potential hackers and other threats. We have deployed industry-standard network security technologies such as firewalls, intrusion detection systems, and anti-virus programs. Additionally, Alltel is in the process of implementing, at substantial cost, security solutions that will encrypt all data stored on laptops and on backup tapes, while encrypting selected data within databases and internal transmissions.

Improvements to Security Processes and Authentication

Alltel has developed and is deploying a robust identity management system designed to ensure that employees and customers gaining access to customer data on-line are properly authenticated. Similarly, Alltel has implemented strict customer authentication requirements for each of the different ways in which customers can access billing system account information, including for information released over the telephone by our call centers, through the Interactive Voice Response (IVR) systems, and at our retail locations. We also have adopted specific verification methods for law enforcement to obtain access to information on an emergency basis.

Many of the security processes currently used to verify customer identity were deployed before the actions of pretexters became widely publicized earlier this year. We continuously refine our processes in response to threat and vulnerability information from a variety of internal and external sources. As an example, in March 2005, we changed our procedures to prohibit our call centers and retail stores from faxing call detail records internally. Alltel policy prohibits the disclosure of call detail information over the telephone, and requires that such information only be sent or faxed to an address or phone number listed on the account prior to the request for account data. Also, Alltel requires subscribers to password protect electronic access to their online accounts and offers customers the additional option of establishing a password to protect against unauthorized access to billing system information by phone or in person.

Alltel recognizes that employees are the first line of defense in protecting customer data against pretexting efforts, and, therefore, Alltel has taken a number of steps to prevent employees from deliberately or accidentally releasing customer phone records to unauthorized persons.

First, an employee's network access is restricted to only the Alltel applications and customer information necessary for the employee to perform his or her job. All Alltel employees and agents agree to abide by the company's information security and confidentiality policies, and receive information security training, including computer-based training on identifying social engineering tactics. Customer service supervisors randomly monitor customer service calls to ensure that customer service employees not only provide good service, but also follow the proper security procedures.

To prevent customer phone records from being released to unauthorized persons impersonating Alltel employees, we have procedures in place to authenticate the identity of Alltel employees and agents prior to allowing them access to customer phone records. We also make our employees aware of pretexting schemes and methods when we become aware of them by placing notices on our employees' online portal and, in some cases, by sending emails to all employees describing recent attempts to procure customer information by fraud. In the rare instance when we do receive a report that an employee has violated Alltel policies, including the Information Security Policy, our internal investigators take immediate action to investigate the allegations. If employees are found to have violated Alltel policies, they are disciplined, and, in some cases, terminated. When warranted, we notify law enforcement of employee violations.

Conclusion

While recognizing that pretexting is a continuing threat to the security of customer data, Alltel notes that data brokers and other persons attempting to obtain unauthorized access to call records use a wide variety of methods to attempt to fraudulently obtain customer data from carriers. Given the demands of customers and the realities of the competitive wireless market, carriers can take steps to prevent pretexting, but will likely not be able to completely stop unauthorized persons from obtaining customer phone records through the use of pretexting any more than a retail store can fully prevent shoplifting. Alltel's position is that legislative efforts should be primarily focused on those who seek to illegally obtain call records, not the carriers who are among the victims of the pretexters' fraud. To that end, Alltel strongly supports the effort by Congress to criminalize the fraudulent actions of the pretexters.

Alltel remains committed to protecting customer information while providing its customers with the highest levels of service. I look forward to continuing to work with the Members of this subcommittee to combat the security threats posed by pretexters. Thank you for the opportunity to testify today.